Document Control	
Date Created	07-Feb-2025
Document Author	Information Security Manager
Date Reviewed	04-Mar-2025
Next Review Date	04-Mar-2026
Current Status	Approved
Date Signed Off	06-Mar-2025
Document Classification	Internal Use Only
Retention Period	Perpetual

Version History

Version	Date	Author	Change History
Version 1.0		ISMS Team	Draft Version
Version 2.0		ISMS Team	Version Review & Update

Distribution List

Name	Version	Date
All Staff	Version 2.0	20th March 2025
ISMS Manager	Version 2.0	20th March 2025
CISO	Version 2.0	20th March 2025

Approval List

Name	Position	Signature	Change History
	CEO		Version 2.0

Change Control

This document is subjected to change control.

Notice

The company will be referred to as “the organization”.

EXECUTIVE SUMMARY

This policy ensures the security of sensitive information by requiring employees to keep workspaces organized and screens protected. The **Clear Desk Policy** mandates securing documents and locking workstations, while the **Clear Screen Policy** requires locking screens and preventing unauthorized viewing. These measures help maintain confidentiality and protect company data.

1.0 SCOPE

This policy applies to all permanent, temporary or contracted staff employed by the organization who can access information.

2.0 POLICY – Clear Desk

To maintain a secure and organized workspace

- Store confidential documents in locked drawers or cabinets when not in use.
- Shred printed materials containing sensitive information when no longer needed.
- Secure external storage devices (USBs, external hard drives) in locked storage.
- Lock laptops and mobile devices with security cables or store them securely.
- Erase sensitive information from whiteboards and shared workspaces before leaving.

3.0 POLICY – Clear Screen

To prevent unauthorized viewing of confidential data:

- Lock your computer screen when away from your desk (Ctrl+Alt+Delete > Lock).
- Set automatic screen locks to activate after a maximum of 5 minutes of inactivity.
- Use privacy filters on screens when working in shared or public spaces.
- Close applications and documents containing sensitive data before stepping away.
- Avoid saving confidential files on desktops; store them in approved secure locations.

4.0 ENFORCEMENT

Violations of this policy may lead to disciplinary action, including restricted access or termination, depending on the severity of the breach. Regular audits will be conducted to ensure compliance